USAFA-DF-PA-293

# The Changing Character of Orientation in *Airpower*

***Thomas A. Drohan and Daniel S. Yinger***

Airpower began with a reputation for thinking ahead of technology. Indeed, the strategic claims of Guilio Douhet and Billy Mitchell were considered outrageous at the time. Imagine aerial bombardment devastating cities and coercing surrender; long-range battleplanes outrunning pursuit aircraft and sinking battleships; and an airpower industry defending the nation and defining its international presence and power. These visionary claims took time to realize, and in varying degrees of success and moral contention. Fortunately, recent airpower theorists, have been, like Mitchell, experienced Airmen who tested innovations in combat. John Boyd's OODA loop, John Warden's concentric rings, and Dave Deptula's effects-based approach to integration operationalized new concepts that improved military performance. Critics charge that such notions over-promise strategic effects. This is true for any approach restricted to single domain analysis, or to only the military aspects of strategy. So airpower needs to be viewed in a broader context, even beyond its own expanding technology.

## *The Need for Strategic Thinking*

Most observers and practitioners today would agree that technology has pulled ahead of traditional concepts of warfare. Complex operations and the limits of a combined arms warfare mindset highlight the need to innovate and develop, rather than simply align with, doctrine. Enter the cyber domain. Cyber is a human-made venue consisting of the binary code generated, processed and distributed by computers, and organized into networks to support the needs of human organizations. While this new domain rests on the bedrock of a physical layer obeying the laws of physics, its syntactic and semantic aspects continuously change as new applications are conceived and developed. Thus cyber has constantly changing rules, and now permeates the air, space, land and maritime *operating* domains. So, classic assumptions about human nature[1] that are applied to war and warfighting domains need to be questioned, and contextualized for cyberspace. This is a challenge to tradition-mired thinking. As in the day of Douhet, prevailing paradigms of warfare and conservative, identity-reinforcing military organizations fail to exploit the full potential of this new operating space. Consider the joint force construct, mandated by the Goldwater-Nichols Department of Defense Reorganization Act of 1986--the only such reform since the National Security Act of 1947.

Despite its reformist bent, the joint force construct is retarded by a combined arms mentality. The intent was to increase joint effectiveness by having the "organize, train and equip" (OT&E)-oriented individual services provide their capabilities to an interdependent joint force. Combatant commands and task forces, then, were supposed to be tailored to the needs of regions and functions, and situations. That happened from a combined arms point of view, but merely combining forces does not equate to planning, programming and combining, much less adjusting, desired effects. Current joint information operations doctrine, for instance, describes "information fires" as if they were effects automatically produced by a cyber arm. Particularly in the cyber domain, we should not assume that we can overwhelm our adversaries with superior arms, "cyber fires," and in so doing, achieve victory. The services' OT&E function needs to connect to broader goals that national leaders want to cause, and prevent. The sheer variety of diplomatic, informational, military, economic and social (DIMES) effects calls for adapting concepts, not just capabilities, when we collaborate. This is a conceptual, technological, and cultural challenge. In this regard, the Air Force's on-going effort to forge a common identity out of its specialized capabilities reflects the creative tension between combined arms and combined effects thinking.

In an attempt to embrace cyber capabilities, Air Force Doctrine Volume 1, Basic Doctrine now defines *airpower* as "the ability to project military power or influence through the control and exploitation of air, space, and cyberspace to achieve strategic, operational, or tactical objectives." Aside from the tautological inclusion of *power* in the new definition, this conceptual integration of air, space and cyber influence across three analytical levels of effects is important. In theory, the broader definition of airpower makes it necessary to distinguish among air, space and cyber influence, operations, and domains. Operations through air, space and cyberspace need to provide influence that is *strategic* from a process perspective. Such integration of multiple domains also holds the potential for a unified Air Force identity if it can replace platform-centric loyalties with a professional bond that values the synergy of airpower. To do this across air, space and cyber domains, we take strategy as a process of coordinating, synchronizing and integrating various ends, ways and means across tactical, operational, and strategic levels of analysis. This means that tactics, operations and strategies need to be understood relative to desired effects. Realistically, this has to be balanced with feasible ways and resourced means.

Bringing cyber capabilities into strategy is a far greater challenge than that for air and space. While the latter are enveloping domains only in a physical sense, cyber affects all physical domains and with even less certainty of results. This becomes clear as we consider how to integrate airpower with land and maritime power in a DIMES-wide strategy. We begin by drawing insights from three modern airpower strategists, and cyber technology. Let's start with John Boyd.

### *Three Airpower Theorists*

Boyd is understood by most as originator of the OODA Loop: Observe, Orient, Decide and Act. Fortunately, Airman-scholar Frans Osinga provides accessible yet rigorous insights into Boyd's larger contributions to airpower and strategy.[2] Osinga's account of Boyd's eclectic perspectives emphasizes the importance of a thought process that is open and disprovable, rather than closed and belief-based. Cyber can enter an open OODA cycle anywhere. By assigning meaning to data as we orient ourselves to our environment, cyber processing affects observation. Fixating on irrelevant data can skew observation. Perceptions influence how we orient ourselves to vast amounts of data, and can alter our attribution of meaning and intent. The semantic manipulation of information in the cyber domain can impact decision making. An adversary may try to reinforce confidence in false information or cast doubt on accurate information; both impact our ability to make a decision. Speeding up the OODA loop, therefore, might worsen our situation rather than improve it. The adage, "never interrupt your enemy while he's making a mistake" applies here. Since orientation involves the filtering of data, information, and perceived reality, it affects the quality of our decisions, how we communicate them through network-centric warfare, and the actions we take. Bad data in cyber is the equivalent of clinging to favored weapons or unexamined doctrine in all conditions. So from Boyd, we conclude that the orientation phase is most important. The willingness to think differently and proactively shape and anticipate new realities, are critical to gaining and maintaining advantage. John Warden applied these attitudes and skills at the level of an air campaign.

Warden's Instant Thunder air campaign plan (1990) for Iraq analyzed the adversary (the Saddam Hussein regime) in terms of functional centers of gravity with strengths and weaknesses.[3] His concentric five-ring model placed leadership at the center, with organic essentials, infrastructure, population, and fielded forces in successively less important outer circles. Since the application of these in Operationn Desert Storm (which included large numbers of ground forces as an adjunct to the air campaign), Warden adapted the framework to suit any organization with identifiable nodes. His modeling of networks with key functions developed targeting into strategy. Drawing from Boyd's psychological and physical isolation of the enemy, Warden advocated simultaneous attacks on vital linkages. If these were vulnerable to airpower, it followed that an enemy's ability and will to resist could be paralyzed. Communications and jamming technologies helped enable manned precision strikes with more rapidity than before, but also led to new vulnerabilities such as dependence. In the cyber domain, competition over strategic materials, goods and services further complicates the operational environment.[4] Human interactions among Warden's rings increasingly are cyber connections. So in targeting an adversary for functional disruption or defending against it, cyber needs to enter each ring to influence the will and/or capabilities of key people and systems. Given the globalization of systems of systems, the need for a coordinated, coherent yet flexible strategy is acute. Dave Deptula broke through this complexity by focusing on the purpose of strategy.

Lt Gen Deptula's articulation of effects-based operations changed the way America can go to war.[5] Like Mitchell, Boyd and Warden, his new ideas were resisted by constituencies asserting the importance of arms over effects. Technology continued to deepen the interdependence of cyberspace with other domains through advances in communications, precision, stealth, and remotely operated systems. Recognizing the reliance of high-tech arms on cyberspace and need for cross-domain dominance, Deptula pressed further. His effects-based approach to operations (EBAO) perspective upended principles of warfare and replaced them with a process for warfare. Mass, for instance, required fewer resources than ever before. So mass was not a fixed combination of arms, but rather an output to be combined with other effects. Information-in-warfare also became a tool of strategy that could create its own effects, rather than serving principles such as surprise or security. Deptula also took on the task of re-organizing a headquarters deputate to actually implement EBAO. He fused intelligence and operations, and intelligence, surveillance and reconnaissance (ISR) functions, by integrating Air Force ISR. This transformation exploited technological developments and operational practices, which broadened orientation and focused campaign planning. Robust interdependence among air, space and cyber operations created symbiotic (both supported and supporting) relationships with a variety of operations. The flexibility enabled rapid decisive operations and led to advanced ISR analysis education and training.

Let's relate some central concepts from Boyd, Warden and Deptula to emerging cyber capabilities. From Boyd, we get the need to maintain adaptation superiority. By this, we mean the relative ability of an individual, group or system to comprehend and exploit dynamic conditions through proactive change. The constant presence of uncertainty underscores why adaptation is critical to survival in a competitive-cooperative world. Warden adds a systems perspective that conceives adversaries in terms of interconnected functions that we can affect simultaneously, in parallel.[6] Deptula focuses on organizing and delivering desired effects...what do we want to achieve? This is the essence of effective strategy that ought to determine choices among ways and means. Now we can imagine how to achieve strategic combinations of preventative and causative effects through systematic adaptation. By exploiting secure, versatile technologies that enhance information assurance and resilient networks in dynamic threat environments, we can program and plan to conduct persistent and pervasive operations. How?

*A Concept of Operations*

One possibility would be to use advances in computer processing, information distribution, intelligence analysis and stealth to create nth-order effects that themselves become tools for further effects. Cyber effects are an order of magnitude more difficult to predict or even anticipate, requiring unprecedented knowledge of enemy systems. Four related capabilities present such opportunities: secure processing, advanced analysis and synthesis, software routing, and low visibility maneuvering in the cyber domain.

Secure processing ensures safe encryption for trusted transmissions in network-penetrated situations, which can deny adversaries the ability to use syntactic-level deception effectively. The systems involved would employ secure-enclave technology. These hardware platforms would have the same physical vulnerabilities as do current systems, with no additional limitations or vulnerabilities beyond what we currently experience. Friendly forces would employ asymmetric advantages in information assurance to communicate and act unimpeded across operating domains. In effect, this would ensure trusted applications in the secure enclave run as expected, however such as systems would still be vulnerable to influences that skew our perceptions (military deception). Solving this still requires developing intelligence and knowledge from data and information.

Collected data and derived information may be academic unless accompanied by the ability to conduct proactive intelligence operations that seize and maintain the OODA initiative. Airmen need to learn advanced analysis that decomposes the operational environment through linkage, pattern, anomaly and aggregation analyses then recomposes it with syntheses based on alternative competing hypotheses. This capability enables us to (a) shape adversary observations of reality, causing him to react to problems of our choosing; and (b) change (and more completely trust) our paradigms more quickly and with more variety to orient ourselves in different situations. This informs our decisions and actions to anticipate and create desired, timed combinations of effects.

Software routing supports these processes by assuring the integrity of friendly data, information and intelligence. Uploaded router brick technology on fixed and mobile platforms would be combined with multiple servers and distributed algorithms to reduce vulnerability to cyber attacks. This would also facilitate collaborative network adaptation in command and control network-centric environments. Smart networks would detect intrusions and share this information with other Network Operation Centers (NOCs). Rapid collaboration could mitigate attacks by allowing the network to rapidly reconfigure itself and provide signature warnings to other NOCs. In addition, mobile secure clouds can deliver cyber effects without network attribution. Stealth airpower platforms that host redundant arrays of sensors, emitters and strikers would lower risks in hostile environments and permit persistent maneuvering of air, space and cyber assets.

The overall increase in network resilience and flexibility to support a wider range of desired effects, demands iterative wargaming, detailed modeling of adversary systems/networks, and advanced intelligence analysis to increase the speed and quality of decision cycles. At the same time, we must identify risks and uncertainty, and take action to minimize those. Warfighters need to express their requirements in more open-ended ways as desired, probabilistic effects, then ways and means developed to achieve them by influencing the will and capabilities of human actors and their perceived conditions. In order to distill what cyber can tell us about combined effects and integrated airpower, we return to our theorists.

*Resilient Orientation*

Boyd's main thrust, to survive in a competitive environment, aims at how we can perceive enemy vulnerabilities. Ignorance of the environment can lead to disorientation and failure to anticipate the need to adapt. In cyberspace, this problem is complicated by distributed competencies and threats on the internet. If an opponent can skew observation and orientation with an attack (virus, worm, Trojan horse, backdoor, denial of service, phishing, spoofing, etc.) , then a faster OODA loop may be a negative factor for us because we can be reacting to the wrong problem. It's more important to learn from mistakes, detect changes, and make adjustments.

If we assume Warden's systemic perspective, we would expect that cyber information can affect enemy decisions if it can enter the leadership ring, where the most influential observations and orientations presumably occur. But in a distributed system such as networks of groups or individuals, however, deconstructing an enemy system is a multi-faceted task, requiring us to identify linkages and nodes that matter most, and those we can affect. The 'fractal' character of Warden's Rings becomes apparent at this point (for instance, the Infrastructure Ring has its own sub-rings of Leadership, Organic Essentials, etc., and so-on). In cyberspace, understanding what the ordered networks are that structure interactions and therefore influence relationships is key to identifying decision points. This can change in a moment, as social networking well illustrates.

Deptula's conceptual and organizational integration of capabilities for desired effects can focus us on what combination of outcomes we want to achieve. This is the non-trivial issue of what's feasible in any given situation as well, given the complexity of service, joint, interagency and coalition environments. When we use cyber tools to create influence, we have to anticipate likely effects and shape desired effects based on networks filled with human and programmed actors and aggregates in various OODA loops. This is a challenging task that requires flatter organizations and more empowered decision-making than some leaders are prepared to permit. All three airpower theorists, however, share this cultural imperative--the need for individuals to re-frame how to make sense of a changing operating environment. As in other complex domains, this applies to cyberspace where predictable behavior quickly becomes a critical vulnerability.

Airpower's operational environment includes multiple OODAs operating among networked platforms and crowd-sourced information that generates huge flows from which to derive intelligence. Mapping these systems requires advanced analysis to identify potential targets and conditions. There are a variety of approaches to modeling effects. Future-casting, for instance, imagines events we want to prevent and cause and back-casts alternative answers to test.[7] Service-specific and joint doctrines have generated procedures for intelligence preparation of the battlespace, but they are too slow for the pace of cyberspace. At a minimum, we need the ability to perceive the operational environment and compare courses of action based on assumptions we make about what cyber systems look like, and how real and virtual  leaders and groups behave.  We need integrity of information just to begin to do this in contested environments. Even if we have more data than an adversary, our advantage in preventing and achieving combined effects requires us to create new understanding. In order to exploit the new potential of airpower, we have to have to stay ahead of existing technologies by investing in our ability for resilient orientation.

[1] Thucydides' elements of human nature and Clausewitz's Trinity, for instance, are routinely invoked to emphasize the doctrinal importance of immutable constants rather than changing characteristics. Commonly mined locations are: Robert B. Strassler, ed., The Landmark Thucydides: A Comprehensive Guide to the Peloponnesian War, (NY: Simon & Schuster, 1996), p. 200; and Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret, ind. ed. (Princeton: Princeton University Press, 1984), p. 89.

[2] Frans Osinga, '*Getting' A Discourse on Winning and Losing: A Primer on Boyd's 'Theory of Intellectual Evolution*, Contemporary Security Policy, 19 Nov 2013, http://www.tandfonline.com/loi/fcsp20.

[3] John A. Warden III, The Air Campaign: Planning for Combat (Washington, D.C.: National Defense University Press, 1988).

[4] See "Cyber Threats" in Department of Defense Strategy for Operating in Cyberspace , July 2011, p. 2.

[5] Brigadier General David A. Deptula, *Effects-Based Operations: Change in the Nature of Warfare* (Arlington: Aerospace Education Foundation, 2001).

[6] Colonel John A. Warden III, *The Enemy as a System*, Airpower Journal  (Spring 1995), pp. 40-55.

[7] Brian David Johnson, Science Fiction Prototyping: Designing the Future with Science Fiction (ebook: Morgan & Claypool, 2011), p. 4.